Elcomsoft iOS Forensic Toolkit

Full version	$ 1995

BUY NOW (/PURCHASE/BUY.

Perform full file system and logical acquisition of iPhone, iPad and iPod Touch devices. Image device file system, extract device secrets (passwords, encryption keys and protected data) and decrypt the file system image.

- Full file system extraction and keychain decryption without a jailbreak
- Logical acquisition extracts backups, crash logs, media and shared files
- Passcode unlock and physical acquisition for legacy devices
- Extracts and decrypts protected keychain items
- Repeatable, forensically sound extraction for select iPhone and iPad models through modified bootloader
- Automatically disables screen lock for smooth, uninterrupted acquisition

Supports: all generations of iPhone, iPad, iPad Pro and iPod Touch, first-generation HomePod; Apple Watch and Apple TV 4 and 4K; all versions of iOS from iOS 4 to iOS 16

Description **Compatible Devices and Platforms** **System requirements**

NEW FEATURES

checkm8 extraction for first-generation HomePod and other Apple devices

iOS Forensic Toolkit 8 for Mac introduces a new extraction method for select iOS devices based on the modified bootloader. The new extraction method is the cleanest yet, enabling repeatable, verifiable extractions and forensically sound workflow.

The HomePod is now fully supported with the forensically sound checkm8 extraction process regardless of the version of iOS installed on the device. Accessing information stored in the first-generation HomePod requires a specific set of tools and steps, including partial disassembly and the use of a custom 3D-printable USB adapter.

HomePod Forensics I: Pwning the HomePod (https://blog.elcomsoft.com/2 forensics-i-pwning-the-homepod/)

HomePod Forensics II: checkm8 and Data Extraction (https://blog.elcomsoft.com/2 forensics-ii-

The forensically sound bootloader-level extraction process is available for multiple Apple devices ranging from the ancient iPhone 4 all the way up to the iPhone X, a large number of iPad, iPod Touch, Apple Watch S3, and Apple TV models. The newly developed checkm8 extraction process supports the widest range of major OS releases in three different flavors (iOS, tvOS, watchOS) for three different architectures (arm64, armv7, armv7k).

Note: checkm8 extraction for the iPhone 8, 8, and iPhone X devices running iOS 16.x only works if no screen lock passcode was ever used since initial setup.

For devices based on the armv7 and armv7k architecture full passcode unlock along with file system extraction and keychain decryption are available. For newer arm64-based devices, full file system extraction and keychain decryption are supported for devices with a known or empty passcode.

Forensic Access to iPhone/iPad/iPod Devices running Apple iOS

Perform the complete forensic acquisition of user data stored in iPhone/iPad/iPod devices. Elcomsoft iOS Forensic Toolkit allows imaging devices' file systems, extracting device secrets (passcodes, passwords, and encryption keys) and accessing locked devices via lockdown records.

The following extraction methods are supported:

- Advanced logical acquisition (backup, media files, crash logs, shared files) (all devices, all versions of iOS)
- Direct agent-based extraction (all 64-bit devices, select iOS versions)
- Forensically sound bootloader-based checkm8 extraction (select devices)
- Jailbreak-based extraction (all devices and versions of iOS with public jailbreaks)
- Passcode unlock and true physical acquisition (select 32-bit devices)

*See **Compatible Devices and Platforms** for details.*

Full File System Extraction and Keychain Decryption

A jailbreak-free extraction method based on direct access to the file system is available for a limited range of iOS devices. Using an in-house developed extraction tool, this acquisition method installs an extraction agent onto the device being acquired. The agent communicates with the expert's computer, delivering robust performance and extremely high extraction speed topping 2.5 GB of data per minute.

Better yet, agent-based extraction is completely safe as it neither modifies the system partition nor remounts the file system while performing automatic on-the-fly hashing of information being extracted. Agent-based extraction does not make any changes to user data, offering forensically sound extraction.

Both the file system image and all keychain records are extracted and decrypted. The agent-based extraction method delivers solid performance and results in forensically sound extraction. Removing the agent from the device after the extraction takes one push of a button.

You can either extract the complete file system or use the express extraction option, only acquiring files from the user partition. By skipping files stored in the device's system partition, the express extraction option helps reduce the time required to do the job and cut storage space by several gigabytes of static content.

checkm8-and-
data-extraction/)

iOS Forensic Toolkit Maintenance: Following Apple iOS Updates
(https://blog.elcomsoft.com/2
forensic-toolkit-
maintenance-
following-apple-
ios-updates/)

iOS 15.5 Low-Level Keychain Extraction
(https://blog.elcomsoft.com/2
15-5-low-level-
keychain-
extraction/)

iOS Forensic Toolkit 8: Apple TV 3, 4, and 4K checkm8 Extraction Cheat Sheet
(https://blog.elcomsoft.com/2
forensic-toolkit-8-
apple-tv-3-4-and-
4k-checkm8-
extraction-cheat-
sheet/)

Elcomsoft End User License Agreement (/Elcomsoft_EULA.pdf)

Installing and signing the extraction agent requires an Apple ID registered in the Apple Developer Program. The Mac edition drops this requirement, allowing to use a regular Apple ID for signing and sideloading the extraction agent onto the iOS device.

Jailbreak-based Extraction

In addition to agent-based extraction, iOS Forensic Toolkit fully supports the extraction of all jailbroken devices for which a jailbreak is available. Full file system extraction and keychain decryption are available for jailbroken devices. All public jailbreaks are supported.

Forensically sound extraction with bootloader exploit

To preserve digital evidence, the chain of custody begins from the first point of data collection to ensure that digital evidence collected during the investigation remains court admissible. The new, bootloader-based extraction method delivers repeatable results across extraction sessions. When using iOS Forensic Toolkit on a supported device, the checksum of the first extracted image will match checksums of subsequent extractions provided that the device is powered off between extractions and never boots the installed version of iOS in the meantime.

The new extraction method is the cleanest yet. Our implementation of bootloader-based exploit is built from the ground up. All the work is performed completely in the RAM, and the operating system installed on the device is not booted during the extraction process. Our unique direct extraction process offers the following benefits:

- Repeatable results. Checksums of subsequent extractions will match the first one if the device is kept powered off and never boots iOS between sessions.
- Supports iPhone 5s, 6/6s/Plus, SE (original), iPhone 7/8/Plus, iPhone X.
- Supports a wide range of Apple models in total including 25 iPhones, 40 iPads, 3 iPods, 4 Apple TV and 4 Apple Watch models
- Wide iOS compatibility. iOS 4 through iOS 16 are supported with limited support for iOS 16 on A11 devices.
- Unaltered system and data partitions.
- Zero data modification policy: 100% of the patching occurs in the RAM.
- The installation process is fully guided and massively more reliable compared to jailbreaking.
- Locked devices supported in BFU mode, while USB restricted mode can be completely bypassed.

Notes: bootloader-level extractions are available exclusively in the Mac edition, requiring a macOS computer.

Unlocking and Imaging Legacy Devices: iPhone 4, 4s, 5, and 5c

Passcode unlock and imaging support are available for legacy iPhone models.

The Toolkit can be used to unlock encrypted iPhone 4, 4s (1), 5 and 5c devices protected with an unknown screen lock passcode by attempting to recover the original 4-digit or 6-digit PIN. This DFU attack works at the speed of 13.6 passcodes per second on iPhone 5 and 5c devices, and takes only 12 minutes to unlock an iPhone protected with a 4-digit PINs. 6-digit PINs will take up to 21 hours. A smart attack will be used automatically to attempt cutting this time as much as possible. In less than 4 minutes, the tool will try several thousand most commonly used passcodes such as 000000, 123456 or 121212, followed by 6-digit PINs based on the dates of birth. With 74,000 of those, the smart attack takes approximately 1.5 hours. If still unsuccessful, the full brute force of the rest of the passcodes is initiated. (Note: passcode recovery runs at the speed of 6.6 passcodes per second on the iPhone 4).

Full physical acquisition is available for legacy iOS devices including the iPhone 4, 4s (1), 5 and 5c. For all supported models, the Toolkit can extract the bit-precise image of the user partition and decrypt the keychain. If the device is running iOS 4 through 7, the imaging can be performed even without breaking the screen lock passcode, while devices running iOS 8 through 10 require breaking the passcode first. For all supported models, the Toolkit can extract and decrypt the user partition and the keychain.

(1) The passcode unlock and forensically sound, checkm8-based extraction are available for the iPhone 4s, iPod Touch 5, iPad 2 and 3 devices via a custom flashed Raspberry Pi Pico board, which is used to apply the exploit. The firmware image is provided with iOS Forensic Toolkit; the Pico board is not supplied.

Notes: Mac edition only; iPhone 4s support requires a Raspberry Pi Pico board (not supplied) with custom firmware (supplied). For iOS 4 through 7, passcode recovery is not required for device imaging. For iOS 8 and 9, the passcode must be recovered before imaging (otherwise, limited BFU extraction available).

Extended Logical Acquisition

iOS Forensic Toolkit supports logical acquisition, a simpler and safer acquisition method compared to physical. Logical acquisition produces a standard iTunes-style backup of information stored in the device, pulls media and shared files and extracts system crash logs. While logical acquisition returns less information than physical, experts are recommended to create a logical backup of the device before attempting more invasive acquisition techniques.

We always recommend using logical acquisition in combination with physical for safely extracting all possible types of evidence.

Quickly extract media files such as Camera Roll, books, voice recordings, and iTunes media library. As opposed to creating a local backup, which could be a potentially lengthy operation, media extraction works quickly on all supported devices. Extraction from locked devices is possible by using a pairing record (lockdown file).

In addition to media files, iOS Forensic Toolkit can extract crash/diagnostics logs and stored files of multiple apps, extracting crucial evidence without a jailbreak. Extract Adobe Reader and Microsoft Office locally stored documents, MiniKeePass password database, and a lot more. The extraction requires an unlocked device or a non-expired lockdown record.

Logical acquisition is available for all devices regardless or hardware generation and jailbreak status. The device must be unlocked at least once after cold boot; otherwise, the device backup service cannot be started.

Experts will need to unlock the device with passcode or Touch ID, or use a non-expired lockdown file extracted from the user's computer.

If the device is configured to produce password-protected backups, experts must use Elcomsoft Phone Breaker (https://www.elcomsoft.com/eppb.html) to recover the password and remove encryption. Elcomsoft Phone Breaker is also required to view keychain records. If no backup password is set, the tool will automatically configure the system with a temporary password ("123") in order to be able to decrypt keychain items (password will be reset after the acquisition).

Using a lockdown (pairing) record, information can be extracted from locked iOS devices even after power-off or reboot. The following matrix applies to devices running iOS 8 and newer:

	Basic device info	Advanced device info	App list	Media	iTunes-style backup
Device locked, no lockdown record	Yes	No	No	No	No
Device never					

unlocked after reboot, lockdown exists	Yes	Yes	No	No	No
Device unlocked after reboot, lockdown exists	Yes	Yes	Yes	Yes	Yes

Supported Devices and Acquisition Methods

iOS Forensic Toolkit implements physical acquisition support for jailbroken devices from iPhone 5s through iPhone 13, 13 Pro, iPhone 13 mini and iPhone 13 Pro Max.

The following compatibility matrix applies:

- **Passcode unlock**: Brute-forces 4-digit and 6-digit screen lock passcodes via DFU exploit. All iOS versions, iPhone 4, 4s, 5 and 5c devices. [1][2]
- **Legacy devices**: Bit-precise imaging and decryption of iPhone 4, 4s, 5 and 5c devices. [1][2]
- **Agent (without a jailbreak)**: Full file system extraction and keychain decryption for devices running iOS 9 through 15.5. The corresponding iPad models are also covered. Apple Developer registration required (Windows)/optional (macOS).
- **With jailbreak**: Physical acquisition for jailbroken devices running any version of iOS for which a jailbreak is available (iPhone 4s through iPhone 12 Pro Max, most iPad models, Apple TV 4 & 4K).
- **Via Bootrom exploit (checkm8)**: Forensically sound file system & keychain acquisition for 76 Apple devices [1]
- **No jailbreak**: Logical acquisition, shared files and media extraction for devices running versions of iOS without a jailbreak. Device must be unlocked with passcode, Touch ID or lockdown record

Perform physical and logical acquisition of iPhone, iPad and iPod Touch devices. Image device file system, extract device secrets (passwords, encryption keys and protected data) and decrypt the file system image.

1. *Only available in the Mac edition.*
2. *iPhone 4s support requires a custom-flashed Raspberry Pi Pico board.*

EIFT. Extract and decrypt iOS keychain

All Features and Benefits

Apple Watch, Apple TV and HomePod Extraction

Keychain Extraction

DFU/Recovery Mode

Video Tutorial

Like 1.7K

Follow @elcomsoft

Buy Elcomsoft iOS Forensic Toolkit

Full version

$ 1995

BUY NOW (/PURCHASE/BUY.PHP?PRODUCT=EIFT&REF=INFOPAGE)

CORPORATE NEWS / ARTICLES

23 March, 2023

Elcomsoft iOS Forensic Toolkit 8.13 adds checkm8 extraction for first-generation HomePod (/news/830.html)

7 February, 2023

Elcomsoft iOS Forensic Toolkit 8.12 adds checkm8 extraction support for iOS 16.3, 15.7.3, and 12.5.7 (/news/829.html)

10 January, 2023

Elcomsoft iOS Forensic Toolkit 8.11 decrypts iOS 15.5

PRESS RELEASES

22 September, 2022

Elcomsoft iOS Forensic Toolkit 8.0 brings forensically-sound checkm8 extraction for select iPhone & iPad models (/press_releases/EIFT_20220922.html)

21 June, 2022

ElcomSoft Brings Forensically Sound checkm8 Extraction to iPad, iPod Touch and Apple TV (/press_releases/eift_20220621.html)

29 April, 2022

ElcomSoft Introduces iPhone 13 File System Extraction keychain (/news/827.html)

29 December, 2022
Elcomsoft iOS Forensic Toolkit 8.10 adds checkm8 extraction for iOS 16.2, fixes extraction agent signing (/news/826.html)

22 September, 2022
Elcomsoft iOS Forensic Toolkit 8.0 brings forensically sound bootloader-based extraction for select iPhone & iPad models (/news/822.html)

Support (/press_releases/eift_20220429.html)

10 February, 2022
ElcomSoft Brings Repeatable, Forensically Sound checkm8 Extraction to iPhone 8, iPhone X and Apple Watch Series 3 (/press_releases/eift_20220210.html)

17 November, 2021
Elcomsoft Brings Repeatable, Forensically Sound Extraction and iOS 15 Support to Select iPhone Models (/press_releases/eift_20211117.html)